Таким образом, можно сделать вывод, что на сегодняшний день самой большой угрозой является терминальный режим, старинные сетевые протоколы, службы, которые никто не использует, но они «кочуют» из дистрибутива в дистрибутив. Разработчикам дистрибутивов стоит провести анализ и убрать лишние пакеты из своих дистрибутивов.

Список литературы

1. Сайт разработчиков ОС Debian. https://www.debian.org.
2. *Корбет Д., Рубини А.* Драйверы устройств Linux // США O'Reilly Media Inc, 2005.

УДК 004.056.2

И. А. Корелин, Т. М. Мкртчян
Научный руководитель: д-р тех. наук, профессор С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ЖИЗНЕОБЕСПЕЧЕНИЕ ЦЕНТРА ОБРАБОТКИ ДАННЫХ: ЗАЩИТА И РИСКИ. ФИЗИЧЕСКАЯ ЗАЩИЩЕННОСТЬ

Аннотация. В статье анализируется несколько вариантов физической защищенности центра обработки данных (ЦОД). Результаты исследования получены на основе системного и процессного подходов. Для оценки результативности исследования автор изучил количественные и качественные методы анализа физической защищенности центра обработки данных. На основе полученных результатов разработаны рекомендации по улучшению качества обслуживания информации, хранящийся на любом электронном носителе. Основная цель физической защищенности — это надежная сохранность любой информации, полученной от клиентов. Также в статье рассматриваются наиболее эффективные и безопасные методы хранения информации. Это позволяет выявлять потенциальных клиентов с помощью ЦОД, обеспечивая необходимые условия для удовлетворения их потребности: сохранности информации.

Ключевые слова: защищенность; процессный подход; услуги; ЦОД; охрана; видеонаблюдение; система; безопасность.

Процесс обмена данными практически полностью перешел в сферу Интернета. Информация стала ценным продуктом на мировом рынке: за сведения о клиентах, конкурентах, своих сотрудниках готовы платить многие компании и частные лица, что увеличивает риск похищения таких данных. Все чаще ЦОД

берут на себя проблемы хранения информации, и эти проблемы становятся все острее. Центр обработки данных — это специализированное помещение для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет.

ЦОД выполняет функции обработки, распространения информации и хранения, в интересах корпоративных клиентов он ориентирован на решение бизнес-задач путем предоставления информационных услуг. Консолидация вычислительных ресурсов и средств хранения данных в ЦОД позволяет сократить совокупную стоимость владения IT-инфраструктурой за счет возможности эффективного использования технических средств [1].

При условии, что у организации есть несколько параметров безопасности, однако, как показано ниже, эти меры часто недостаточны.

Самый сбалансированный способ — обеспечить физическую безопасность центров обработки данных, т. е. внедрить многоуровневую защиту (несколько параметров безопасности). Как защита эшелона прорыв одного уровня не будет означать прорыва системы безопасности. В этом случае безопасность внутреннего периметра не менее важна, чем внешнего, что позволяет снизить риск внутренних угроз, а также непредвиденных вредоносных операций. Согласно опросу, проведенному 600 финансовыми экспертами в Нью-Йорке и Лондоне, 25 % пользователей признали, что они не смогут использовать внутреннюю информацию для своих целей независимо от последствий, большинство из них знают о незаконности своих действий. Таким образом, страхи работодателей и их 69 % пользователей представляют наибольшую угрозу для их деятельности в штате.

Большинство владельцев центра обработки данных знают о необходимости контроля доступа к информации, однако игнорируют разницу в доступе к ЦОД. Часто можно обнаружить ситуацию, связанную с тем, что центр обработки данных имеет защищенный периметр, доступ к объекту строго ограничен, но вот проход в машинный зал открыт для всего обслуживающего персонала, а работник, не зная, может создать опасную ситуацию, что может привести к остановке центра обработки данных.

Вопреки представлению многих клиентов ЦОД, средства обеспечения безопасности не ограничиваются системами, которые поддерживают хакерские атаки, хакерами и другими методами получения несанкционированной информации. Существует также проблема с физической безопасностью центров обработки данных, так как она должна обеспечивать безопасность информации о клиентах в своих компьютерных комнатах. Причем, в отличие от организации информационной безопасности телекоммуникационных сетей, которая должна соответствовать законодательству и нормативным требованиям РФ (это, например, Федеральный закон № 149-ФЗ от 27 июля 2006 г., Указ

Президента Российской Федерации от 17 марта 2008 г. № 351, Постановление Правительства № 531 от 31 августа 2006 г.), физическая защита ЦОД практически полностью передается в ведение его оператора, поэтому клиент встает перед ответственной задачей: правильно выбрать надежный дата-центр для хранения своей информации.

Проблемы безопасности центров обработки данных очень важны с точки зрения обслуживания клиентов. В целом их можно разделить на две основные группы: физическую безопасность центра данных и его юридическую защиту.

Физическая защищенность

Основной целью физической защиты центра обработки данных является предотвращение несанкционированного доступа к информации, хранящейся на серверах клиента. Уже при строительстве дата-центра большое внимание следует уделять организации безопасности и контроля доступа на своей территории, включая контрольно-пропускные пункты, камеры видеонаблюдения, механизмы заказа на вход и так далее. Основные аспекты организации физической системы безопасности:

- **Охрана объекта.** Оператору ЦОД необходимо ответственно подойти к выбору охранного предприятия. В соответствии с законодательством РФ частные охранные предприятия (ЧОП) вправе оказывать профессиональные услуги в области охраны объекта, в том числе с применением огнестрельного оружия. Взаимодействия с профессионалами в сфере службой безопасности снижает риск утечки информации. Во время выбора предприятия оператор ЦОД должен уделять пристальное внимание тому, каким образом службы безопасности работают на рынке, сколько частных служб безопасности уже работает, доступны ли требуемые лицензии и разрешения, текучесть кадров в прошлом году и т. д. Оператор центра обработки данных сможет справиться с возможными проблемами, связанными с объектами.
- **Видеонаблюдение**. Вся площадь центра обработки данных и прилегающей территории полностью должны охватываться системой видеонаблюдении. Поскольку центр обработки данных постоянно работает, а клиенты и поставщики доступны круглосуточно, система мониторинга должна быть организована не только службой безопасности, но и долговременной видеозаписью. Премиум сервисный центр нуждается только в больших системах видеонаблюдения для видеонаблюдения, необходимости дополнительного архивирования и длительного хранения до 5 лет видеозаписей, что позволяет оператору ЦОД, его клиентам и поставщикам услуг быстро восстанавливать любые события дня. Этот уровень видеозаписи неизбежен в дата-центре во время нелицензионных тестов доступа.

– **Системы обеспечения безопасности**. Вход в здание и немедленный доступ к компьютерным комнатам центра обработки данных должен включать несколько уровней защиты. Теперь наиболее распространенные системы защиты используют биометрические данные посетителей (отпечатки пальцев, живопись и т. д.).

Надежность центра обработки данных также повышается за счет подключения к мощным противопожарным дверям и дверям шин.

В дополнение к защите здания оператор центра обработки данных ограничивает доступ к области, прилегающей к центру обработки данных. Для этого следует использовать надежные ограждения с противовоспалительной защитой.

Повседневная работа сопровождается природными факторами, например, тепло, вода и коррозия. Однако для защиты прав пользователя на раскрытие программы строительство ЦОД до сих пор абсолютно внимания не уделяется [2].

Список литературы

1. https://www.osp.ru/lan/2013/10/13037914
2. http://telecombloger.ru/3418

УДК 004.056.53

С. Д. Субботин
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ДОПОЛНИТЕЛЬНЫЕ ПРОГРАММНО-АЛГОРИТМИЧЕСКИЕ СРЕДСТВА УСИЛЕНИЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ БАНКОМАТА

Аннотация. В статье рассмотрено устройство банкомата и его актуальные уязвимости. Данное исследование имеет целью выработку рекомендаций и предложений, направленных на усиление существующей защиты банкомата с целью снижения вероятности взлома и хищения из него денежных средств. Безопасность платежных терминалов и противодействие корыстным преступлениям представляет собой важное направление в деятельности финансовых и правоохранительных органов.

Ключевые слова: банкомат; защита; идентификация; визуальное изображение; распознавание; обнаружение; OpenCV.